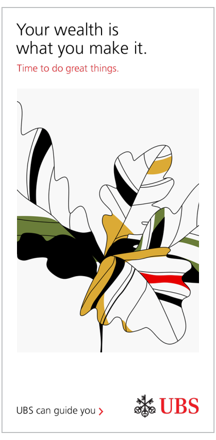
ANDY GREENBERG SECURITY 09.06.2017 06:00 AM

Hackers Gain Direct Access to US Power Grid Controls

Hackers who hit American utilities this summer had the power to cause blackouts, Symantec says. And yes, most signs point to Russia.

GETTY IMAGES


Your wealth is
what you make it.
Time to do great things.
UBS can guide you ›
UBS

IN AN ERA of hacker attacks on critical infrastructure, even a run-of-the-mill malware infection on an electric utility's network is enough to raise alarm bells. But the latest collection of power grid penetrations went far deeper: Security firm Symantec is warning that a series of recent hacker attacks not only compromised energy companies in the US and Europe but also resulted in the intruders gaining hands-on access to power grid operations---enough control that they could have induced blackouts on American soil at will.

Symantec on Wednesday revealed a new campaign of attacks by a group it is calling Dragonfly 2.0, which it says targeted dozens of energy companies in the spring and summer of this year. In more than 20 cases, Symantec says the hackers successfully gained access to the target companies' networks. And at a handful of US power firms and at least one company in Turkey---none of which Symantec will name---their forensic analysis found that the hackers obtained what they call operational access: control of the interfaces power company engineers use to send actual commands to equipment like circuit breakers, giving them the ability to stop the flow of electricity into US homes and businesses.

"There's a difference between being a step away from conducting sabotage and actually being in a position to conduct sabotage ... being able to flip the switch on power generation," says Eric Chien, a Symantec security analyst. "We're now talking about on-the-ground technical evidence this could happen in the US, and there's nothing left standing in the way except the motivation of some actor out in the world."

Never before have hackers been shown to have that level of control of American power company systems, Chien notes. The only comparable situations, he says, have been the repeated hacker attacks on the Ukrainian grid that twice caused power outages in the country in late 2015 and 2016, the first known hacker-induced blackouts.

The Usual Suspects

Security firms like FireEye and Dragos have pinned those Ukrainian attacks on a hacker group known as Sandworm, believed to be based in Russia. But Symantec stopped short of blaming the more recent attacks on any country or even trying to explain the hackers' motives. Chien says the company has found no connections between Sandworm and the intrusions it has tracked. Nor has it directly connected the Dragonfly 2.0 campaign to the string of hacker intrusions at US power companies---including a Kansas nuclear facility---known as Palmetto Fusion, which unnamed officials revealed in July and later tied to Russia.

Chien does note, however, that the timing and public descriptions of the Palmetto Fusion hacking campaigns match up with its Dragonfly findings. "It's highly unlikely this is just coincidental," Chien says. But he adds that while the Palmetto Fusion intrusions included a breach of a nuclear power plant, the most serious DragonFly intrusions Symantec tracked penetrated only non-nuclear energy companies, which have less strict separations of their internet-connected IT networks and operational controls.

As Symantec's report on the new intrusions details, the company has tracked the Dragonfly 2.0 attacks back to at least December of 2015, but found that they ramped up significantly in the first half of 2017, particularly in the US, Turkey, and Switzerland. Its analysis of those breaches found that they began with spearphishing emails that tricked victims into opening a malicious attachment---the earliest they found was a fake invitation to a New Year's Eve party---or so-called watering hole attacks that compromise a website commonly visited by targets to hack victims' computers.

Those attacks were designed to harvest credentials from victims and gain remote access to their machines. And in the most successful of those cases, including several instances in the US and one in Turkey, the attackers penetrated deep enough to screenshot the actual control panels for their targets' grid operations---what Symantec believes was a final step in positioning themselves to sabotage those systems at will. "That's exactly what you'd do if you were to attempt sabotage," he says. "You'd take these sorts of screenshots to understand what you had to do next, like literally which switch to flip."

ADVERTISEMENT

And if those hackers did gain the ability to cause a blackout in the US, why did they stop short? Chien reasons that they may have been seeking the option to cause an electric disruption but waiting for an opportunity that would be most strategically useful---say, if an armed conflict broke out, or potentially to issue a well-timed threat that would deter the US from using its own hacking capabilities against another foreign nation's critical infrastructure. "If these attacks are from a nation state," Chien says, "one would expect sabotage only in relation to a political event."

The Ukrainian Precedent

Not every group of hackers has shown that kind of restraint. Hackers now believed to be the Russian group Sandworm used exactly the sort of access to electricity control interfaces that Symantec describes Dragonfly having to shut off the power to a quarter million Ukrainians in December 2015. In one case they took over the remote help desk tool of a Ukrainian energy utility to hijack engineers' mouse controls and manually clicked through dozens of circuit breakers, turning off the power to tens of thousands of people as the engineers watched helplessly.

Operations like that one and a more automated blackout attack a year later have made Russia the first suspect in any grid-hacking incident. But Symantec notes that the hackers mostly used freely available tools and existing vulnerabilities in software rather than previously unknown weaknesses, making any attribution more difficult. They found some Russian-language strings of code in the malware used in the intrusions, but also some hints of French. They note that either language could be a "false flag" meant to throw off investigators.

Related Stories

INFRASTRUCTURE
Senators Push Trump for Answers on Power Grid Malware Attack
ANDY GREENBERG

SECURITY
Feds' Smart Grid Race Leaves Cybersecurity in the Dust
KIM ZETTER

INFRASTRUCTURE
Squirrels Keep Menacing the Power Grid. But at Least It's Not the...
BRIAN BARRETT

In naming the hacking campaign Dragonfly, however, Symantec does tie it to an earlier, widely analyzed set of intrusions also aimed at the US and European energy sectors, which stretched from as early as

2010 to 2014. The hackers behind that series of attacks, called Dragonfly by Symantec but also known by the names Energetic Bear, Iron Liberty, and Koala, shared many of the same characteristics as the more recent Dragonfly 2.0 attacks, Symantec says, including infection methods, two pieces of malware used in the intrusions, and energy sector victims. And both the security firm Crowdstrike and the US government have linked those earlier Dragonfly attacks with the Kremlin---a report published by the Department of Homeland Security and the FBI last December included the group on its list of known Russian-government hacking operations.

Symantec says it has assisted the power companies that experienced the deepest penetrations, helping them eject the hackers from their networks. The firm also sent warnings to more than a hundred companies about the Dragonfly 2.0 hackers, as well as to the Department of Homeland Security and the North American Electric Reliability Corporation, which is responsible for the stability of the US power grid. NERC didn't immediate answer WIRED's request for comment on Symantec's findings, but DHS spokesperson Scott McConnell wrote in a statement that "DHS is aware of the report and is reviewing it," and "at this time there is no indication of a threat to public safety."

But Symantec's Chien nonetheless warns any company that thinks it may be a target of the hackers to not only remove any malware it has identified as the group's calling card but also to refresh their staff's credentials. Given the hackers' focus on stealing those passwords, even flushing all malware out of a targeted network might not prevent hackers from gaining a new foothold if they still have employees' working logins.

The Dragonfly hackers remain active even today, Chien warns, and electric utilities should be on high alert. Given that the group has, in some form, been probing and penetrating energy utility targets for the past seven years, don't expect them to stop now.

Andy Greenberg is a senior writer for WIRED, covering security, privacy, and information freedom. He's the author of the book *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. The book and excerpts from it published in WIRED won a Gerald Loeb Award for... Read more

SENIOR WRITER

Featured Video

WATCH
Watch How Hackers Took Over a Ukrainian Power Station

Watch How Hackers Took Over a Ukrainian Power Station

Watch as hackers take over the mouse controls of Ukrainian grid operators, part of a breach that caused a blackout for a quarter million people.

TOPICS HACKERS POWER GRID

News of the future, now.
Get WIRED
SUBSCRIBE

WIRED

WIRED is where tomorrow is realized. It is the essential source of information and ideas that make sense of a world in constant transformation. The WIRED conversation illuminates how technology is changing every aspect of our lives—from culture to business, science to design. The breakthroughs and innovations that we uncover lead to new ways of thinking, new connections, and new industries.

MORE FROM WIRED
Subscribe
Newsletters
FAQ
Wired Staff
Press Center

CONTACT
Advertise
Contact Us
Customer Care
Send a tip securely to WIRED
Jobs

RSS | Site Map | Accessibility Help | Condé Nast Store | Condé Nast Spotlight COOKIES SETTINGS

© 2020 Condé Nast. All rights reserved. Use of this site constitutes acceptance of our User Agreement (updated 1/1/20) and Privacy Policy and Cookie Statement (updated 1/1/20) and Your California Privacy Rights. *Wired* may earn a portion of sales from products that are purchased through our site as part of our Affiliate Partnerships with retailers. The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast. Ad Choices